

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-115
of 1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

REPLY COMMENTS OF SPRINT NEXTEL CORPORATION

Kent Y. Nakamura
Frank P. Triveri
Anthony M. Alessi
Edward J. Palmieri
Sprint Nextel Corporation
2001 Edmund Halley Drive
Reston, VA 20191

Douglas G. Bonner
Kathleen Greenan Ramsey
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005
(202) 408-6400

Counsel for Sprint Nextel Corporation

Dated August 7, 2007

SUMMARY

A majority of commenting parties agree that the Commission should await full implementation of the recently adopted new rules and take into account carrier and customer experiences alike before considering additional customer proprietary network information ("CPNI") requirements. Millions of Sprint Nextel customers and those of other carriers will be affected greatly by the implementation of the new rules that the Commission adopted earlier this year. Imposing additional requirements on carriers at this time will undermine current compliance efforts. Carriers are expending tremendous resources to effectively implement new compliance regimes on time and in a way that minimizes negative impacts to the customer experience. Additional requirements at this critical juncture will further complicate that fragile process.

Several commenting parties, including Sprint Nextel, have shown how the proposed additional requirements for which the Commission has sought comment will (1) not eliminate or reduce pretexting, (2) provide no measurable benefit to justify the additional confusion and complexity with which customers would have to cope, and (3) impose considerable financial and operational burdens on carriers. The Commission should not rush to impose any additional requirements on carriers, but should instead first weigh the impact of the implementation of its new CPNI rules on pretexting activities, while allowing carriers to complete the substantial authentication system changes for all customers that the new rules will require. In view of the fast approaching December 2007 deadline to implement the new CPNI rules, additional rules now would create more onerous operational and financial burdens that are likely to undermine and harm carrier-customer relationships.

TABLE OF CONTENTS

SUMMARY	i
I. EXPANDED PASSWORD PROTECTION FOR NON-CDR CPNI WILL NOT ENHANCE PROTECTION OF CPNI AND WILL FRUSTRATE CUSTOMERS.....	4
II. AN AUDIT TRAIL REQUIREMENT WILL NOT ENHANCE PRIVACY PROTECTION FROM PRETEXTERS.	7
III. CARRIERS NEED FLEXIBILITY TO IMPLEMENT THE MOST EFFECTIVE PHYSICAL SAFEGUARDS.....	8
IV. LIMITING DATA RETENTION WOULD BE ADVERSE TO THE PUBLIC INTEREST.	11
V. NEW RULES TO PROTECT CUSTOMER INFORMATION STORED IN MOBILE DEVICES ARE UNWARRANTED.....	14
VI. A COMPREHENSIVE OPT-IN POLICY WOULD FAIL TO ADDRESS PRETEXTING AND VIOLATE 47 USC § 222 AND THE CONSTITUTION.	17
VII. CONCLUSION.....	21

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-115
of 1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

REPLY COMMENTS OF SPRINT NEXTEL CORPORATION

Sprint Nextel Corporation ("Sprint Nextel"), through its undersigned counsel, respectfully submits its reply comments to the comments filed in response to the Commission's Further Notice of Proposed Rulemaking released on April 2, 2007, in the above-captioned proceedings.¹ Additional CPNI rules are premature at this time. There is a clear consensus among commenters that the most prudent course is to refrain from imposing additional rules until implementation of the recently adopted CPNI rules has been completed, and the Commission, carriers and customers have had adequate

¹ *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115 and WC Docket No. 04-36, Further Notice of Proposed Rulemaking (rel. April 2, 2007) ("*Further NPRM*").

opportunity to assess their effectiveness.² Carriers already have a lot to do to prepare for the new CPNI rules that are scheduled to take effect on December 8, 2007. As AT&T recommends, carriers “should be afforded a reasonable opportunity to implement [the recently adopted] requirements before any new requirements are considered.”³

Not only are additional rules premature, they appear unnecessary. Many commenters agree that expanding the CPNI rules to include additional measures, such as password protection of non-CDR CPNI, is unwarranted.⁴ New CPNI rules that impose new audit trail requirements, inflexible physical safeguards, and data retention limitations that fail to account for carriers’ legitimate business needs for data would (1) not address pretexting, (2) harm the carrier-customer relationship, and (3) impose costs on carriers that would far exceed any corresponding benefit. The combination of the criminalization of pretexting under the recently enacted Telephone Records and Privacy Protection Act,⁵

² See e.g., Comments of AT&T Inc. at 2 (filed July 9, 2007) (“AT&T Comments”); Comments of Comcast Corporation at 1-2 (filed July 9, 2007) (“Comcast Comments”); Comments of COMPTTEL at 1 (filed July 9, 2007) (“COMPTTEL Comments”); Comments of Embarq at 1-2 (filed July 9, 2007) (“Embarq Comments”); Comments of the National Cable & Telecommunications Association at 2 (filed July 9, 2007) (“National Cable & Telecommunications Ass’n Comments”); Comments of the National Telecommunications Cooperative Association at 2 (filed July 9, 2007) (“National Telecommunications Cooperative Ass’n Comments”); Joint Comment of NuVox Communications and XO Communications, LLC at 2 (filed July 9, 2007) (“Joint Comments”); Comments of Time Warner Inc. at 2-3 (filed July 9, 2007) (“Time Warner Comments”); Comments of T-Mobile USA, Inc. at 2-3, 9 (filed July 9, 2007) (“T-Mobile Comments”); Comments of the United States Telecom Association at 2 (filed July 9, 2007) (“USTA Comments”) and Comments of Verizon at 1-2 (filed July 9, 2007) (“Verizon Comments”).

³ AT&T Comments at 2.

⁴ See e.g., AT&T Comments at 2-4; Comments of Qwest Communications International Inc. at 4-5 (filed July 9, 2007) (“Qwest Comments”); Time Warner Comments at 3-5; and Verizon Comments at 1-2.

⁵ Telephone Records and Privacy Protection Act of 2006, Pub.L. No. 109-476, 120 Stat.

increased carrier protection of CPNI, and current and new CPNI protections make any further CPNI regulation unnecessary.⁶

Only two among approximately twenty-nine commenting parties support more regulation of CPNI by the Commission, as contemplated by the *Further NPRM*. These are the comments submitted by the “Consumer Coalition”⁷ and the New Jersey Division of Rate Counsel (“NJ DRC”).⁸ The Consumer Coalition asks the Commission to adopt additional rules to: (1) expand password protection to all CPNI; (2) require carriers to maintain audit trails; (3) require carriers to implement additional internal physical safeguards, including encrypting all CPNI data and limiting employee access; (4) limit carrier data retention; (5) require carriers to safeguard information stored by customers in cell phones; (6) curtail law enforcement related delay of customer notification of security breaches; and (7) require a comprehensive opt-in policy.⁹ The NJ DRC seeks the

3567 (Jan. 12, 2007) (codified at 18 U.S.C. § 1039).

⁶ One commenter notes that the need for additional rules protecting CPNI has already declined substantially since the Commission first initiated the rulemaking in this proceeding on February 14, 2006 given the new CPNI rules and the enactment of the Telephone Records and Privacy Protection Act. Comments of MetroPCS Communications, Inc. at 2 (filed July 9, 2007) (“MetroPCS Comments”) (“In short, since the Commission first opened the record in this proceeding, the risk of pretexting has diminished considerably, while the penalties for and consumer protections against pretexting have multiplied.”).

⁷ Comments of: Consumer Action, Consumer Federal of America, Consumers Union, Electronic Privacy Information Center, national Consumers League, Privacy Activism, Privacy Journal, Privacy Rights Clearinghouse, U.S. Public Interest Research Groups, Utility Consumers’ Action Network (filed July 9, 2007) (“Consumer Coalition Comments”).

⁸ Comments of the New Jersey Division of Rate Counsel (filed July 9, 2007) (“NJ DRC Comments”).

⁹ Consumer Coalition Comments at 1.

extension of password protection rules to all CPNI, limitation of the law enforcement related delay of customer notice, and further consideration of the feasibility and costs associated with consumer ability to delete or transfer CPNI when new phones are purchased.¹⁰ More consumer protections always sound appealing, but the Commission must consider these recommendations in light of the services that customers need and demand. As explained below, the recommendations and requests of the Consumer Coalition and the NJ DRC will not address the problem of pretexting or unauthorized access to CPNI. More likely, their recommendations would significantly frustrate customers and result in consequences contrary to the public interest.

I. EXPANDED PASSWORD PROTECTION FOR NON-CDR CPNI WILL NOT ENHANCE PROTECTION OF CPNI AND WILL FRUSTRATE CUSTOMERS.

Many commenting parties agree that either restricting or complicating consumer access to non-CDR CPNI data such as minutes used to date in a particular month - information that is of no interest to pretexters but of significant interest to consumers - is not in the public interest.¹¹ Specifically, password protection of non-CDR CPNI could be expected to: (1) frustrate customers by hindering and, in some instances, blocking entirely their ability to access non-CDR CPNI; (2) prevent customers from paying bills; (3) prevent customers from making informed choices about new rate plans; (4) frustrate the carrier-customer service relationship; (5) fail to deter in any meaningful way pretexter

¹⁰ NJ DRC Comments at IV-VI.

¹¹ See e.g., AT&T Comments at 5; Verizon Comments at 2-8 (“Removing that limitation [of password protection to the disclosure of CDR information] and requiring customers who call a center to provide a password before a carrier discloses *any* CPNI would cause the burden of the CPNI regulations on carriers and customers to be overwhelming.”).

and data broker activities, and (6) overwhelm carrier call centers already receiving significant volumes of customer service calls each day, rendering such call centers unavailable to many consumers.

Customers demand efficient and convenient fulfillment of their customer service needs. Sprint Nextel strives to meet those customer needs as quickly as possible – preferably through self service options or a quick, one-time telephone call. Obligatory passwords for non-CDR CPNI would frustrate these customer expectations and carrier goals. As the Commission noted, “many customers may not like passwords” and “passwords...can be lost or forgotten.”¹² The Commission also recognized that passwords place a burden on carriers seeking to provide prompt customer service and on customers seeking ready access to account information.¹³ Expanded password requirements for non-CDR CPNI would ignore these concerns.

Commenting parties point to third party research that confirms Commission observations that customers may dislike and often forget passwords.¹⁴ It is also apparent

¹² *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115 and WC Docket No. 04-36, Report and Order, paras. 13 n.45 and 16 (rel. April 2, 2007) (“Order”).

¹³ *Order* at para. 17.

¹⁴ *See*, Larry Ponemon, “Perceptions About Passwords,” BNA Privacy and Security Law Report (March 6, 2006) (88 percent of people surveyed had forgotten their password at least once in the previous two years; 67 percent forgot their passwords at least three times in the prior two years); *see also* Verizon Comments at 5 (discussing other surveys); AT&T Comments at 5 (“study after study has shown that customers do not like to use passwords, and those who do often forget them, rendering them ineffective as a regulatory tool.”); T-Mobile Comments at 4 (“no evidence in the record that data brokers have any interest in non-CDI associated with customer accounts.”). One commenter suggests that the notion that customers do not like passwords is “simplistic” and “lack[s]

that customers who do not access their carrier accounts as frequently as they access their bank ATM accounts will more often forget their password, leading to substantially increased customer frustration.¹⁵ Furthermore, there is no reason to expand password protection and disrupt customers' quick and convenient access to non-CDR CPNI because non-CDR CPNI is not relevant to pretexters. Contrary to Consumer Coalition claims, there is simply no "loophole for pretexters to exploit."¹⁶ In fact, there is no record of abuse of non-CDR information that supports requiring passwords.

Similarly, expanded password requirements for non-CDR CPNI would increase call handling time, equally frustrating carriers and millions of customers. Many customers will likely find it difficult to immediately obtain the information they require to pay bills, monitor usage of services to stay within budget, and make decisions about upgrading or downgrading rate plans. The Commission should not underestimate the

any empirical support" (NJ DRC Comments at V), but this clearly is not the case given the recognized studies in this area.

¹⁵ US Telecom Ass'n Comments at 3 (customers call customer service "only occasionally and often cannot remember passwords" and "most customers do not want passwords for customer service calls"); Verizon Comments at 5-6 (Verizon states that "nearly three million" attempted logins by residential online account users "fail or are abandoned" per year by users who cannot supply (or retrieve by answering a test question) a correct password.).

¹⁶ Consumer Coalition Comments at 7. The Consumer Coalition provides no evidence or examples of such a loophole. Furthermore, password protection for access to any form of customer CPNI will not involve "minimal training" as the Consumer Coalition argues. *Id.* Comprehensive training would be necessary to ensure that thousands of customer care representatives require password disclosure for all routine CPNI requests, assist livid customers who have forgotten passwords with re-setting their passwords, and do not inadvertently reveal CPNI that is incidental to fulfilling the purpose for the customer's service call. See Comments of Sprint Nextel Corporation at 4 (filed July 9, 2007) ("Sprint Nextel Comments") (discussing the estimated 130,000 hours of training for 34,000 customer care representatives to deploy Sprint Nextel's automated customer authentication solution for its Uniform Billing Platform ("UBP")).

importance to customers of promptly concluding such transactions. A password requirement for non-CDR CPNI could effectively block these transactions in the moment of need with no corresponding benefit, except to create irate customers and undermine the carrier-customer experience.¹⁷

Sprint Nextel urges the Commission not to adopt rules mandating that consumers use a password for access to non-CDR CPNI. Instead, the Commission should allow carriers to tailor the appropriate level of protection to non-CDR CPNI by balancing the sensitivity of the information in question with the convenience to that information demanded by customers.

II. AN AUDIT TRAIL REQUIREMENT WILL NOT ENHANCE PRIVACY PROTECTION FROM PRETEXTERS.

The Consumer Coalition argues that audit trails “aid prosecution of pretexters.”¹⁸ However, the Coalition does not offer any examples of how audit trails actually do so. The fact is that an audit trail system that tracks each and every question asked by a customer service representative during the course of an inbound call would not identify a pretexter. It would not prevent a pretexter from illegally obtaining CPNI. Nor would it uncover one. If a pretexter has the correct authentication credentials, an audit trail will indicate only that information was provided during an apparently legitimate transaction and identify which employee accessed the account. This information is of scant value in identifying pretexting, and does not assist law enforcement in criminal pretexting

¹⁷ Verizon Comments at 8 (Verizon estimates for example that “upwards of 20 million” of its customers do not have passwords and would be need to issued one in the event passwords are mandated for routine customer access to non-CDR CPNI.).

¹⁸ Consumer Coalition Comments at 8.

investigations.¹⁹ In fact, Sprint Nextel's experience shows that law enforcement authorities rarely subpoena audit trails in criminal investigations.

Carriers use audits as part of a larger network security program when it makes sense to do so and when the audits add value. Because network security necessarily involves a holistic approach by carriers involving numerous security variables, regulators should not attempt to micromanage carriers by imposing audit trail requirements.²⁰ Additionally, the costs of implementing extensive audit trails across different systems are considerable, especially when measured against their inability to prevent unlawful pretexting. Using precious resources for these measures cannot be justified when there is no evidence that audit trails will assist in the prosecution of pretexters.

III. CARRIERS NEED FLEXIBILITY TO IMPLEMENT THE MOST EFFECTIVE PHYSICAL SAFEGUARDS.

The Consumer Coalition asks the Commission to "require carriers to encrypt stored CPNI."²¹ In support of this position, the Consumer Coalition points to the Federal Trade Commission ("FTC") recommendation that businesses "consider" encrypting sensitive information stored on networks, disk, laptops and portable storage devices.²² The FTC does not require encryption. The Consumer Coalition also argues that "a number of major carriers already employ encryption protocols for transmission of

¹⁹ Sprint Nextel Comments at 9-10 (law enforcement authorities "rarely subpoena" audit trails in criminal investigations).

²⁰ See also Qwest Comments at 9.

²¹ Consumer Coalition Comments at 10.

²² *Id.*

information and when customers view their data online,”²³ and that new encryption requirements simply would be a “reasonable extension of carriers’ preexisting practices.”²⁴

Sprint Nextel uses encryption as a part of its overall network security approach, where it is necessary, effective and efficient to deploy, but not as a cure-all for all security needs. While the Consumer Coalition is correct in its general observation that Sprint Nextel uses encryption technology when customers view their data online,²⁵ Sprint Nextel does not take a haphazard approach to deploying encryption strategies. Rather, it strategically deploys encryption technology only where effective.²⁶ Like other carriers, Sprint Nextel also utilizes perimeter defenses, policing, alarms, and encryption to prevent and detect unauthorized access. This mix of defenses varies, depending on the information’s sensitivity and its location in the Sprint Nextel information-technology (IT) infrastructure.

For instance, it often does not make sense to use encryption when data is in storage. When in storage, the data is deep within the network perimeter on dedicated servers with compensating security measures such as tight access controls and encrypted

²³ *Id.*

²⁴ *Id.*

²⁵ Consumer Coalition Comments at 10 and n.45.

²⁶ As discussed in detail in its initial comments, Sprint Nextel ensures the security and confidentiality of CPNI through a series of reinforcing safeguards, including restricting access, and implementing a series of IT security measures such as firewalls and intrusion detection systems. Special protections have been implemented for storage and transmission of billing system data. And Sprint Nextel continuously reassesses its technology and processes to ensure that the security of customer data remains robust and state-of-the-art. Sprint Nextel Comments at 13-15.

access credentials. It also may not make sense because access speed to customer records on these systems is necessary to provide quick and reliable customer service. Thus, encrypting this highly secure information would amount to overkill, degrading performance as the information is decrypted each time it is accessed. This degradation of performance would translate to intolerable wait times for customers as calls pile up in the queue. On the other hand, Sprint Nextel utilizes encryption where it makes sense. For example, Sprint Nextel uses its encryption gateway whenever it transfers sensitive data of any kind to its vendors. The information comes out of storage and is encrypted prior to transit.

As shown above, it is inaccurate to suggest that use of encryption throughout carrier networks is universal or necessary. It is also a misconception that encryption can simply be scaled upwards with the turn of a dial. And it is overly simplistic to conclude that the absence of encryption throughout a network means that the network is less secure. Sometimes there is a need to store information in unencrypted format. When there is this need, robust compensating controls are used.

Encryption can be a good solution, but not for every circumstance. It has also been shown that it is important for each carrier to have the flexibility to make its own strategic network security deployment decisions. Even the FDIC interagency banking guidelines do not require encryption for sensitive financial information in all circumstances. Banking guidelines only suggest to financial institutions that encryption be used where there is reason and only in some situations.²⁷

²⁷ <http://www.fdic.gov/regulations/information/ebanking/66FR8615.pdf> (see pp. 8621,

As for Sprint Nextel, network management makes reasoned and holistic network security determinations as to when it is best to encrypt CPNI. Where Sprint Nextel has sensitive information that is, by design, stored without encryption, it uses alternative compensating security controls. Sprint Nextel is confident that these network security alternatives are secure.

IV. LIMITING DATA RETENTION WOULD BE ADVERSE TO THE PUBLIC INTEREST.

Commenting parties almost unanimously oppose the proposed data retention limitation.²⁸ Their position is well founded. There is no evidence in the record that a data retention limitation period would in any way diminish pretexting. In fact, the record demonstrates that not only would any data retention limitation be meaningless in addressing pretexting, it would harm the public interest by: (1) interfering with regulatory compliance requirements and tax audits; (2) complicating resolution of billing and contractual disputes subject to state statutes of limitation; and (3) imposing

8630); *see also*, Federal Trade Commission, Protecting Personal Information: A Guide for Businesses (The FTC recommends, but does not require, encryption.); *see also*, the FTC Safeguard Rule - <http://www.ftc.gov/os/2002/05/67fr3685.pdf>.

²⁸ *See e.g.*, Comments of Alexicon Telecommunications Consulting at 4 (filed July 9, 2007) ("Alexicon Comments"); Comments of American Association of Paging Carriers at 3 (filed July 9, 2007) ("American Association of Paging Carrier Comments"); AT&T Comments at 8; Comcast Comments at 8; COMPTTEL Comments at 2; Embarq Comments at 4; Comments of ICORE, Inc. at 3 (filed July 9, 2007) ("ICORE Comments"); Comments of the Iowa Telecommunications Association at 6 (filed July 9, 2007) ("Iowa Telecom Ass'n Comments"); MetroPCS Comments at 10; National Cable & Telecommunications Ass'n Comments at 4; National Telecommunications Ass'n Comments at 2-3; Joint Comments at 7; Qwest Comments at 13; Comments of Rural Cellular Association at 5 (filed July 9, 2007) ("Rural Cellular Ass'n Comments"); Time Warner Comments at 11; T-Mobile Comments at 7; USTA Comments at 6; Comments of USA Mobility, Inc. at 11 (filed July 9, 2007) ("USA Mobility Comments"); and Verizon Comments at 17.

significant costs on carriers and diverting carrier resources without any corresponding benefit.

Requiring data deletion or data de-identification after a specified period of time would not prevent nor effectively reduce the unauthorized disclosure of CPNI because the most highly valued CPNI sought by the data brokers who purchase such records is that which is most recent.²⁹ All evidence demonstrates that pretexters use low-tech means and seek recent information.³⁰ There is no evidence that such criminals would seek, or benefit from, somewhat older consumer data.³¹

In support of an unspecified data retention limitation, the Consumer Coalition argues that personally identifiable information should be eliminated by carriers as soon as it is no longer needed.³² At the same time, the Coalition recognizes that personally identifiable information is “widely available” from other non-carrier sources.³³ Somewhat differently than the Consumer Coalition, Sprint Nextel believes that data should be kept for as long as there is a business or legal need to maintain the data. Sprint

²⁹ Bob Sullivan, *Who's Buying Cell Phone Records Online? Cops*, MSNBC (May 1, 2006), <http://www.msnbc.msn.com/id/12534959/>.

³⁰ Sprint Nextel Comments at 17.

³¹ AT&T Comments at 8 (“In AT&T’s experience, these unscrupulous parties want to know who customers are calling now, not a year or two ago.”)

³² Consumer Coalition Comments at 13-14 (“[P]ersonally identifiable information, such as Social Security numbers, account numbers, billing information and contact lists are targets for identity thieves and should be eliminated as soon as the information is no longer needed for billing or a dispute. Likewise, calling history, the location of the caller, and calendar and speed dial data are vulnerable to misuse by stalkers, harassers and domestic abusers and should be eliminated as soon as such data is no longer needed for billing or a dispute.”).

³³ Consumer Coalition Comments at 4.

Nextel also believes that there is not a full appreciation of why carriers maintain CPNI and other data for particular time periods. Carriers keep this information as necessary to facilitate the following: (1) investigations of alleged wrongdoing; (2) prosecution or defense of allegations of unlawful behavior; (3) resolution of billing disputes; (4) resolution of commercial disputes; (5) compliance with tax laws; (6) defense of breach-of-contract claims; (7) protection of carrier rights and property; and (8) compliance with the data retention rules and regulations.

A broad requirement that carriers destroy data could conflict with the law and frustrate goals that, on balance, further the public interest. For instance, statutes of limitation periods for breach of contract vary by state—as much as five years or more, thus necessitating corresponding data retention schedules. The Commission requires carriers to maintain billing records for 18 months.³⁴ The Commission also requires contributors to the federal Universal Service Fund to maintain certain supporting records and documentation for three years.³⁵ Various legal or tax “holds” can require that records be retained even longer. Qwest reports that necessary retention periods may range, in its experience, from seven to fifteen years.³⁶

In short, the reasons for maintaining customer information are part of a complicated calculus. Carriers have every incentive to maintain this information only so

³⁴ 47 C.F.R. § 42.6.

³⁵ 47 C.F.R. § 54.711(a).

³⁶ Qwest Comments at 13.

long as is necessary, as data storage is expensive.³⁷ And, as the Commission can see, carrier data retention practices further the public's interest in protecting rights and property and complying with the law. Accordingly, the Commission must refrain from imposing indiscriminate data retention obligations on carriers.

V. NEW RULES TO PROTECT CUSTOMER INFORMATION STORED IN MOBILE DEVICES ARE UNWARRANTED.

The record demonstrates that the imposition of rules to secure customer information stored in mobile communications devices is impractical and unnecessary. Importantly, none of the information (*e.g.* songs, photographs and address books) stored on a handset is CPNI and thus is not addressed by section 222 of the Act.³⁸ There is no legal obligation imposed on carriers to protect information stored in handsets. And, as previously explained in Sprint Nextel's comments, and supported by commenting parties,³⁹ the consumer chooses what data to access, use, and store on a wireless device

³⁷ It was recently reported that the Federal Bureau of Investigation ("FBI") is also seeking congressional authorization for \$5 million annually to defray the costs incurred by carriers in retaining customer data required by the FBI in counterterrorism investigations. *FBI Seeks to Pay Telecoms for Data*, Ellen Nakashima, Washington Post (July 25, 2007). <http://www.washingtonpost.com/wp-dyn/content/article/2007>.

³⁸ Sprint Nextel Comments at 20-22.

³⁹ Alexicon Comments at 4 ("consumers must take personal responsibility for protection of any personal information they may store in mobile communications devices."); AT&T Comments at 9 ("Carriers do not typically have access to such information and play no role in determining what information a consumer chooses to store on mobile devices or how that information is used. Indeed, in some respects, mobile communications devices are becoming more like computers, laptops, personal digital assistants and other devices that permit customers to store their information." Customers are in the "best position to know what data they have stored on their mobile devices and to take responsibility for safeguarding and erasing that information before disposal or recycling the device."); Embarq Comments at 5 ("customers will have to take some steps to protect their own privacy." It is "no different than what individuals have to do to protect their other private information."); and Iowa Telecommunications Ass'n Comments at 7 ("mobile equipment is almost exclusively the property of the customer....").

and is responsible for protecting the information. For example, most wireless devices allow the consumer to activate a password lock, protecting the device from unauthorized access.

Although the information on mobile devices is not CPNI, carriers still take steps to help customers protect their data. As such, the Commission need not impose any new requirements on carriers - the industry has already voluntarily taken steps to protect wireless customers.⁴⁰ For example, Sprint Nextel's wireless phone recycling program, "Sprint Project Connect,"TM accepts many makes and models of wireless handsets, regardless of the carrier who sold the handset or served the customer.⁴¹ Sprint Project Connect'sTM website recommends to consumers that they "erase personal data" prior to making any donation, providing a link to consumers for free access to a "Cell Phone Data Eraser" tool via WirelessRecycling.com.⁴² This tool provides consumers with step-by-step instructions for removing their personal information for virtually any make or model handset. This publicly available information, in addition to other manufacturer-provided tools and information, is available to all consumers. Commenting parties also have

⁴⁰ No commenting party advocates a requirement that carriers remove customer information at the customer's request on the carriers' premises. As previously explained in Sprint Nextel's Comments, it is simply unworkable and cost prohibitive. Sprint Nextel Comments at 23.

⁴¹ Donated wireless phones are refurbished and resold or their components are recycled. Net proceeds are contributed to 4NetSafety, a Sprint-sponsored program in partnership with the National Center for Missing & Exploited Children and the NEA Health Information Network. See, http://www.sprint.com/citizenship/communities_across/project_connect_faqs.html#faq1.

⁴² http://www.wirelessrecycling.com/home/data_eraser/ The Cell Phone Data Eraser tool is part of a comprehensive national recycling program designed and launched by CTIA and its member companies. AT&T Comments at 11.

illustrated several additional examples of manufacturer-provided handset programs or tools and other recycling programs that enable customers and carriers to remove stored information.⁴³

In addition to the personal data removal functions available to wireless handset users, as the Consumer Coalition points out, Sprint Nextel also offers its business customers a “kill service,” which enables them to send a signal to a handset to remotely delete all data on the device if it is lost or stolen.⁴⁴ Given these industry solutions, the imposition of costly and burdensome requirements on carriers - a one size fits all approach - is unwarranted.

There is no evidence in the record that existing industry solutions described above are not working or do not meet customers’ needs. As MetroPCS points out, incidents of released consumer data from handsets appear to occur when the carrier is not even involved (*e.g.*, the customer sells the handset on eBay without first removing his/her personal information in accordance with manufacturer instructions.).⁴⁵ In fact, the single incident cited by the Consumer Coalition, a test conducted by Trust Digital, involved handsets purchased through eBay.⁴⁶ While the incidents of obtaining consumer data from

⁴³ AT&T Comments at 9; Embarq Comments at 5; American Ass’n of Paging Carriers Comments at 4; T-Mobile Comments at 8.

⁴⁴ The kill service is offered as part of a bundled telecommunications management business solution service called “Sprint Managed Mobility Services,” designed for and typically purchased by medium and large business customers. *See*, http://nextelonline.nextel.com/en/solutions/managed_services/security_services.shtml.

⁴⁵ MetroPCS Comments at 11.

⁴⁶ Consumer Coalition Comments at 15. Sprint Nextel customers are not obligated legally to return their handsets to Sprint Nextel. In fact, customers have various options

handsets purchased on eBay are a concern, consumers must be reminded to be careful when disposing of their handsets - just as consumers must evaluate the appropriate method of disposing other equipment with stored personal data, like personal computers.⁴⁷ That is a matter for continued public education and personal responsibility, not carrier regulation. Without ample evidence that current industry solutions are not working, there is no basis or justification for imposing burdensome new requirements on carriers.

In sum, it is impractical to impose any obligations given the vast amounts of information that may be stored by, and shared among, consumers. There is no basis for such an obligation under Section 222. Moreover, given the industry solutions currently in place, the imposition of costly and burdensome requirements on carriers - a one size fits all approach - is unwarranted. Accordingly, there is no basis or justification for a mandatory rule.

VI. A COMPREHENSIVE OPT-IN POLICY WOULD FAIL TO ADDRESS PRETEXTING AND VIOLATE 47 USC § 222 AND THE CONSTITUTION.

The Consumer Coalition requests that the Commission require carriers to obtain opt-in consumer consent for any and all types of use of CPNI.⁴⁸ However, implementing

once finished with their handset. Customers may donate their handsets to charity, keep the handsets, store the handsets, discard the handset or, as demonstrated in the record, sell the handset. *See* Sprint Nextel Comments at 20.

⁴⁷ As MetroPCS points out, “[t]here is undoubtedly more private data on computers than on cell phones and other wireless equipment, yet there is *no requirement* that computer manufacturers provide an option to securely erase data from their products. Laptop and desktop computers are regularly discarded or refurbished, leaving data on those devices no less vulnerable than data on cell phones and the like.” MetroPCS Comments at 11 (emphasis added).

⁴⁸ *Id.*

such a regulation would require violating Section 222—the statute that underlies the CPNI regulations. It is well settled that Section 222(c)(1) authorizes carriers to use, disclose or permit access to CPNI to market to that customer telecommunications services in the same category of services to which the customer already subscribes, without obtaining prior express approval.⁴⁹ This is known as the total service approach (“TSA”).

Specifically, the Commission found that customers expect that CPNI generated from their use of the service will be used by their carrier to market improved services within the parameters of the carrier-customer relationship; moreover, this expectation is rooted in the statute itself.⁵⁰ Consequently, a draconian and comprehensive opt-in regime, as the Consumer Coalition advocates, would on its face upend the well-settled understanding of Section 222.

⁴⁹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (“CPNI TSA Order”), subsequent history omitted, see also, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*; Clarification Order and Second Further Notice of Proposed Rulemaking, 16 FCC Rcd 16506 (2001) (“CPNI Clarification Order”); see also, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*; Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, para. 83 (2002) (“Third CPNI Order”).

⁵⁰ CPNI TSA Order at paras. 23, 24 and 35.

Moreover, it would violate the Constitution. On August 18, 1999, the United States Court of Appeals for the Tenth Circuit issued an opinion vacating the Commission's opt-in customer approval rules, finding that they impermissibly regulated protected commercial speech and thus violated the First Amendment.⁵¹ The Court found that the opt-in regime was not narrowly tailored because other options, less burdensome on free speech, were not fully considered.⁵² Subsequently, the Commission released its *Third CPNI Order* on in July, 2002, and stated clearly its interpretation of Section 222(c) (1): Congress intended that a carrier may use CPNI without customer approval to deliver and market services within the TSA.⁵³

In urging an expansive application of the opt-in approval requirement going far beyond what the Commission adopted in its April, 2007 *Order*, the Consumer Coalition provides no authority for disturbing this body of Commission precedent upholding a carrier's use of CPNI under the well-established total service approach. Additionally, the Consumer Coalition does not demonstrate how its recommendation to expand the opt-in approval requirement to any transfer of CPNI satisfies the test for restricting commercial speech under the First Amendment.⁵⁴

In addition to violating Section 222, First Amendment rights, and impeding the consumer benefits that flow from the TSA, the opt-in requirement would negatively

⁵¹ *US WEST v. FCC*, 182 F.3d 1224, 1239 (10th Cir. 1999).

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Order* n.138, citing *Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980).

impact carriers and their customers. The fact is that opt-in consumer approval would amount to a prohibition on carriers' ability to use CPNI to develop newer technologies and services, and would impede a customer's ability to receive tailored offerings of services that meet their individual, continuing, and evolving needs. For example, the wireless customer might never learn about a more cost-effective and advantageous service plan, or about emerging wireless technologies like wireless broadband that might appeal to them based on certain customer uses of existing telecommunications services. These costs and burdens to the carrier-customer relationship resulting from a comprehensive opt-in policy resulting from the Consumer Coalition's proposal would offer no offsetting benefits.⁵⁵

In fact, as the Commission knows, there is no nexus between the opt-in regime that the Consumer Coalition advocates and the pretexting activity that gave rise to this preceding. An overbroad opt-in regime simply would not have prevented the thievery perpetrated by pretexters, who rely on low-tech social-engineering to trick customer-service representatives into giving out customer information.

Consequently, the Commission should not extend further its CPNI opt-in rules.⁵⁶ Doing so would raise serious statutory and Constitutional issues, and would not enhance customer privacy in any way.

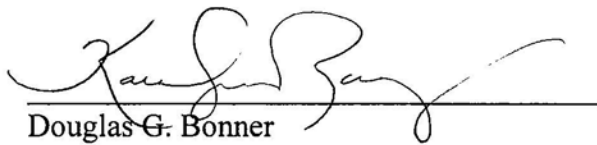
⁵⁵ The Consumer Coalition suggests that, as an alternative to its comprehensive opt-in policy, carriers inform each customer repeatedly of the identity of every affiliate and agent. Given the current parameters for sharing CPNI and the customer expectations in certain circumstances, as established in prior Commission orders, such a requirement is unnecessary and would only serve to unfairly burden carriers and customers with onerous, repetitive reports.

⁵⁶ 47 C.F.R. §64.2007(b); *see also*, *Order* at 37 (expanding opt-in requirement).

VII. CONCLUSION

The protection of CPNI is a serious issue, and is clearly one where the telecommunications industry already has strong incentives to self-police. As discussed herein, Sprint Nextel believes that the *Order*, together with existing CPNI regulations and carriers' own safeguards, sufficiently protect CPNI without additional Commission rules. Given carriers' current systems and network management security regimes, the complexity and variety of carrier billing systems, and customers' demand for convenient access to information, it is best to allow carriers maximum flexibility in determining the best way to protect against unauthorized access to non-CDR CPNI. Additionally, customer information on mobile communications devices is not CPNI, and carriers are not in the best position to guarantee the privacy and security of information contained on these devices. Finally, an expansion of the CPNI opt-in rules would fail to address pretexting and would raise serious questions of statutory authority and constitutionality.

Respectfully submitted,



Kent Y. Nakamura
Frank P. Triveri
Anthony M. Alessi
Edward J. Palmieri
Sprint Nextel Corporation
2001 Edmund Halley Drive
Reston, VA 20191

Douglas G. Bonner
Kathleen Greenan Ramsey
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005
(202) 408-6400

Counsel for Sprint Nextel Corporation

Dated August 7, 2007